IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

SRI INTERNATIONAL, INC., a California Corporation, Plaintiff and Counterclaim-Defendant, v. INTERNET SECURITY SYSTEMS, INC., a Delaware corporation, INTERNET SECURITY SYSTEMS, INC., a Georgia corporation, and SYMANTEC CORPORATION, a Delaware corporation, Defendants and Counterclaim-Plaintiffs.	C. A. No. 04-1199 (SLR) **REDACTED**

SRI INTERNATIONAL, INC.'S RESPONSE TO SYMANTEC'S SUMMARY JUDGMENT MOTION OF NON-INFRINGEMENT

Dated: June 30, 2006

FISH & RICHARDSON P.C.

John F. Horvath (#4557)
Kyle Wagner Compton (#4693)
919 N. Market St., Ste. 1100
P.O. Box 1114
Wilmington, DE 19889-1114
Telephone: (302) 652-5070
Facsimile: (302) 652-0607

Howard G. Pollack (CA Bar No. 162897)
Katherine D. Prescott (CA Bar No. 215496)
500 Arguello St., Ste. 500
Redwood City, CA 94063
Telephone: (650) 839-5070
Facsimile: (650) 839-5071

Attorneys for Plaintiff and Counterclaim Defendant
SRI INTERNATIONAL, INC.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

I. INTRODUCTION

Symantec's accused products practice every limitation of the asserted claims of the '203, '615, and '212 patents, as evidenced by the documents and deposition testimony, and as summarized by SRI's technical expert, Dr. George Kesidis, in his Report on Infringement. Symantec's main non-infringement argument with respect to these patents – that the accused products are not "monitors" – is entirely based on its proposed claim construction, which improperly and selectively imports features of the preferred embodiment into the claims. If Symantec's proposed construction is rejected, its summary judgment motion seeking noninfringement on this ground must be denied.

Symantec's other non-infringement argument relating to the '203, '615, and '212 patents is that SRI has allegedly not provided sufficient evidence of *use* of one category of accused products, the "Manager" products in combination with the SGS series of "sensors," in order to establish that there has been direct infringement. But Symantec fails to appreciate that more than one third of the asserted claims of these patents are *apparatus* claims for which actual use by customers is not required to prove infringement. Moreover, Symantec ignores the evidence establishing its own infringing use of the products and the strong circumstantial evidence of further direct infringement by its customers.

The evidence also establishes that those claims of the '615 and '212 patents requiring a "statistical detection method" of analyzing network data for suspicious activity are also infringed. Symantec argues non-infringement, however, on the tenuous theory that if a "threshold" is used in any way in the analysis, the detection technique must be signature-based and not statistical. But both Dr. Kesidis and ISS' expert Dr. Staniford agree that a threshold comparison can comprise a "statistical detection method" when either the threshold itself *or* the quantity being compared to the threshold is statistically derived. Thus, use of a threshold in and of itself is not determinative of whether the method using the threshold is "statistical" or "signature-based." SRI has

provided substantial evidence that the accused Symantec products, in fact, employ statistical detection methods and this evidence is more than sufficient to compel denial of summary judgment.

The evidence also supports a finding that Symantec's REDACTED performs the building and comparing of long-term and short-term statistical profiles required by the claims of the '338 patent. At the very least, there are *bona fide* factual disputes because the evidence in Symantec's own documentation and source code supports the reasonable inference that the claim limitations are satisfied, and SRI's expert has opined that they are. There are, thus, genuine issues of material fact as to this infringement question that must be considered and decided by the jury.

II. ARGUMENT

A. *Legal standard for summary judgment.*

Summary judgment is only appropriate where "there is no genuine issue as to any material fact and ... the moving party is entitled to a judgment as a matter of law." FED. R. CIV. P. 56(C). *See also Applied Med. Res. Corp. v. U.S. Surgical Corp.*, 448 F.3d 1324, 1331 (Fed. Cir. 2006). All evidence presented by the non-movant is to be taken as true and all reasonable inferences must be drawn in the non-movant's favor. *Adickes v. S. H. Kress & Co.*, 398 U.S. 144, 157 (1970).

B. Symantec's primary non-infringement argument as to the '203 and '615 patents relies entirely on its improper claim construction.

Documentary and testimonial evidence establishes that Symantec's REDACTED products infringe every asserted claim of the '203 and '615 patents, as do Symantec's

REDACTED

Kesidis explained in his report, the accused network monitor products detect suspicious

activity in accordance with the asserted claims.[1] Even though the evidence supports a finding of literal infringement, Dr. Kesidis also explained that the accused products also infringe under the doctrine of equivalents.[2]

Should the Court adopt SRI's proposed construction of "monitor" and "network monitor," infringement is basically uncontested.

REDACTED

But Defendants' proposed "monitor" construction is legally flawed insofar as it attempts to import the limitations of "generic code" and "reusable modules" into the claims. The claims themselves simply recite a network monitor, and do not by their terms require either "generic code" or "reusable modules." As explained in SRI's claim construction briefing (D.I. 265 and D.I. 266 and contemporaneous filings), there is no justification in the claims, specification, or the file history to import any features of the preferred embodiment into the claims, let alone the particular features that Defendants have selected. To the extent Symantec's motion is based on a legally incorrect claim construction of network monitor and hierarchical monitor, it should be denied.

C. The accused Symantec products employ "statistical detection methods" as required by certain asserted claims.

SRI has provided substantial evidence that the accused products meet all the limitations of the asserted claims of the '212 patent and claim 7 of the '615 patent, including the statistical detection requirement. Based on his analysis of Symantec's own documents, including source code for the accused products, and the deposition testimony

---

1 *See* Ex. A, Kesidis Report on Infringement at ¶¶ 64-71, 134, 209. Unless otherwise specified, Exhibits referenced in this responsive brief are attached to the supporting declaration of Kyle Wagner Compton.

2 *See* Ex. A, Kesidis Report on Infringement at ¶¶ 74-76, 133.

3 The only exception is claim 7 of the '615 patent, which requires a statistical detection method and which is addressed below.

REDACTED

of Symantec's technical witnesses, Dr. Kesidis provided and explained in his Infringement Report a specific example of how the accused products invoke statistical detection methods.[4] In particular, he explained that

REDACTED

Ex. B at 13:31-49 (teaching calculating a ratio or percentage of SYN requests and SYN_ACK responses as one example of a statistical detection method)]. Consistent with Dr. Kesidis' opinions, Symantec's own documents REDACTED

REDACTED [*See, e.g.*, Ex. C,

(emphasis added); Ex. D,

REDACTED

(emphasis added)] Even Symantec's expert, Jeffery Hansen, concedes that the

REDACTED

[*See* Ex. E The percentage at issue in this instance ***is*** a basic statistical construct and comparing this statistically derived quantity to a threshold may be a statistical detection method, even when the threshold is "fixed."

The sole basis for Symantec's motion of non-infringement related to "statistical" detection, is the flawed assertion that *any* comparison of network data to a "fixed" threshold is necessarily a signature-based comparison and, therefore, not a statistical technique. The use of thresholds, however, is not confined to signature-based

REDACTED

[4] *See generally,* Ex. A, Kesidis Report on Infringement at ¶¶ 64-69, 142 (explaining that the accused products practice the claimed statistical detection method.)

[5]

REDACTED

approaches. [Kesidis Decl. ¶¶ 16-18]. Thresholds may also be used in statistical detection methods.[6] For example, the quantity being compared to the threshold could be a statistically determined quantity such as the ratio of acknowledged SYN requests to unacknowledged SYN requests in a statistically significant sample of packet traffic data. [*See* Kesidis Decl. ¶ 16]. Or, the threshold itself could be statistically determined. [*See* Kesidis Decl. at ¶ 16]. The testimony of Phillip Porras, a named inventor, is consistent. [*See* Ex. F, at 339:25-340:23 (explaining that threshold comparison techniques may sometimes be considered as a form of signature analysis, and may in other circumstances be considered statistical analysis techniques)]. In his expert report and deposition testimony, one of ISS's experts explained that

REDACTED

[Ex. G, Ex. H, . Thus there is substantial evidence confirming that statistical detection techniques may involve the use of thresholds.

Symantec, however, attempts to argue otherwise. Symantec relies on a sound-bite from Dr. Kesidis' deposition, regarding a misguided hypothetical concerning a threshold comparison in a totally irrelevant context, and tries to leverage this testimony into an "admission" that all detection methods involving threshold comparisons are necessarily not statistical. But Dr. Kesidis made no such broad concession. Failed login attempts, the subject of Symantec counsel's hypothetical questions, are inherently suspicious and, as such, it has been long-recognized that a mere count of such events suffices to detect suspicious activity requiring further analysis or attention.[7] [Kesidis Decl at ¶ 17]. The

---

[6] Indeed, as explained in SRI's claim construction briefing, Defendants' own constructions admit that thresholds are used in the long-term/short-term profile comparisons described in the specification, which they agree are statistical in nature.

[7] Dr. Kesidis explained during his deposition that signature analysis is characterized by detecting activity that was previously determined to be suspicious, whereas statistical detection methods are capable of identifying suspicious activity that has not previously been observed. [Ex. I, at 480:12-481:4].

patents' specification explicitly lists failed login attempts as one of a number of specific event types that give rise to suspicion merely by occurring more than a small threshold number of times.[8] [Ex. B, at 7:43-54]. Nowhere in his expert report did Dr. Kesidis opine that failed login attempts are detected using a statistical detection method, either as described in the patent or as employed in any accused product. [*See generally* Ex. A]. Dr. Kesidis, in fact, explained during his deposition that detecting failed login attempts with a simple threshold analysis is simply irrelevant to the claimed statistical detection method. [*See* Ex. I, at 483:19-485:1 (explaining that statistical detection methods are appropriate where individual network packets are innocuous in and of themselves, and distinguishing failed login attempt detection based on a simple, fixed-threshold comparison, as a type of signature-based alert generation.)]. Looking at all of the deposition evidence, and not just the snippet Symantec has quoted, shows at a minimum that whether use of a threshold can occur in the context of a statistical detection method is at the very least disputed.

Furthermore, even ignoring, *arguendo*, the statistical quality of REDACTED REDACTED a factual dispute remains as to another, independent use Symantec makes of statistical detection. As described below, the evidence shows that the REDACTED also uses a statistical detection method. Thus, several material factual dispute exists as to whether the accused products include one or more statistical detection methods. Drawing all reasonable inferences from this evidence in favor of SRI, Symantec's motion for summary judgment of non-infringement should be denied as to the asserted '212 patent claims and claim 7 of the '615 patent.

---

[8] In fact, all of the examples given in the patent as lending themselves to "rudimentary, inexpensive signature analysis"—fingers, pings, or failed login requests to accounts such as guest, demo, visitor, anonymous FTP, or employees who have departed the company (Ex. B, at 7:50-54)—are events that, as individual occurrences, would be considered innately suspicious by a security professional. As such, a very simple threshold count can be used to determine if further action is warranted when dealing with such unique events. *See* Ex.B, at 7:50-54; Kesidis Decl. at ¶ 17.

D. Symantec's argument regarding evidence of actual deployment of the accused products ignores the distinction between method claims and apparatus claims and also ignores the evidence.

SRI has adduced evidence of direct infringement by Symantec's own, internal deployment of the accused products.[9] SRI has also shown Symantec's inducement and contribution to direct infringement by its customers.[10] Other than its claim construction argument disposed of above, Symantec does not substantively dispute how its products function or that the accused products practice the claims of the hierarchy patents when used as intended. Symantec's sole argument is that SRI has allegedly not provided sufficient proof of actual "use" of the accused network monitors. Insofar as it alleges a want of actual proof of "use," Symantec's motion should be denied on several grounds.

First, it is worth noting that Symantec's argument regarding proof of actual use does not extend to the Manhunt Group of accused products,

REDACTED

Symantec's "use" argument, thus, relates to only some of the accused products.

Second, REDACTED Symantec's argument fails to appreciate the distinction between apparatus claims and method claims.[11] Symantec's argument improperly attempts to import an additional limitation into the apparatus claims: a method step requiring "using" the SGS network monitors with the manager products. [Symantec Br. at 24-29].[12] But infringement of apparatus claims

---

9 *See* Ex. A, Kesidis Report on Infringement at ¶¶ 56-59.

10 *See* Ex. A, Kesidis Report on Infringement at ¶¶ 56-58, 60-63.

11 Thirty out of the eighty claims asserted against the SGS Group of products are apparatus claims ('212 patent claims 14-23, '203 patent claims 12-20 and 22, and '615 patent claims 13-21 and 23). The remaining fifty asserted claims are method claims ('212 patent claims 1-11 and 13, '203 patent claims 1-9 and 11, and '615 patent claims 1-10, 12, 34-41, 43-51, and 53). (The SGS Group of products are not accused of infringing the ten asserted claims of the '338 patent.)

12 "Symantec Br." refers to Symantec's Opening Brief in Support of its Summary Judgment of Non-Infringement (D.I. 286).

requires only that the infringing structure be found. *See, e.g., Cyrix Corporation v. Intel Corporation*, 846 F.Supp. 522, 536 (E.D. Tex. 1994) ("To infringe an apparatus claim, it is not necessary for an accused device actually to be performing the functions specified by the claim. All that is required is that the device have the claimed structure, and that this structure in the device have the *capability* of functioning as described by the claim.") (emphasis in original), *citing Intel Corp. v. U.S. Intern. Trade Com'n*, 946 F.2d 821, 832 (Fed.Cir.1991). Symantec infringed the asserted claims as soon as it sold the monitor and manager products, which, when sold to the same customer, demonstrably contain every structural limitation of the apparatus claims. For example, there is and can be no dispute that the accused manager products

[*See* Ex. J,

REDACTED

Ex. K,

Ex. L

There is also no dispute that capable of "detecting suspicious network activity based on an analysis of network traffic data selected from" the categories recited in, for example, '203 patent claim 12. Because these products collectively provided by Symantec to customers are capable of functioning in the system of the claims, these apparatus claims are directly infringed when Symantec provides these capabilities to its customers, regardless of how the customers, in fact, use them.

Third, at a minimum, a factual dispute exists because there is evidence of actual sales[14] **REDACTED** to

---

[13] *See, e.g.*, '203 patent claim 12, '615 patent claim 13 and '212 patent claim 14.

[14] Symantec repeatedly refused to provide customer information associated with its sales of the accused products, based on a variety of excuses. Although it had no basis to refuse this production and it ultimately did produce some customer data, Symantec

individual customers. By providing these products to the same customer, even if provided in separate "sales," Symantec is providing a "system" that includes the capabilities recited in all the limitations of the claims. Symantec cannot avoid liability for infringement of an apparatus claim by providing the necessary parts separately, if there is no requirement in the claims that the parts necessarily must be used together, rather than be "adapted" to be capable of collective use.

REDACTED

[*See* Ex. M,

Although this evidence does not directly show

REDACTED it provides circumstantial evidence that Symantec's customers do, in fact, use the different products they purchase from Symantec together in their actual network deployments REDACTED

Fourth, as to the asserted method claims, which do require use to practice the method steps, SRI has discovered evidence of direct infringement REDACTED

REDACTED SRI has discovered direct evidence that deploys its products as intended in a network environment,

REDACTED

---

did not provide this sales information until May 26, 2006, in its Seventh Supplemental response to SRI's Interrogatory No. 17, nearly a month after the submission of SRI's expert's report on infringement. Symantec should not be allowed to leverage its discovery abuses into an argument that SRI lacks evidence that was uniquely in Symantec's possession this entire case.

[*See* Ex. N

REDACTED

[*See* Ex. O

[Ex. P,

Furthermore, circumstantial evidence exists that supports the proposition that Symantec customers directly infringe the method claims. After all, that is why they buy these Symantec products. For instance, as discussed above, the evidence shows that

Ex. Q,

REDACTED

Ex. R,

At the current summary judgment stage in the proceedings, the reasonable inference should be drawn that customers actually used the products they purchased. *See Adickes*, 398 U.S. at 157. The inference of actual deployment by customers finds further support in evidence showing that

. [Ex. S,

REDACTED

Thus, a factual dispute exists as to whether Symantec products were actually deployed and used as claimed by the asserted

method claims. Drawing all reasonable inferences in SRI's favor, Symantec's motion should be denied.

REDACTED

E. The performs long-term and short-term statistical profiling and thus infringes the claims of the '338 patent.

Substantial evidence has also been discovered showing that REDACTED practice the "statistical profile" limitations, and thereby infringe the asserted claims of the '338 patent. As Dr. Kesidis explained in his expert report –Symantec incorrectly calls this a "new infringement theory[15]" first raised in deposition–

REDACTED

Indeed, the totality of the evidence from Symantec's technical documents,

---

15

REDACTED

[*See, e.g.*, Ex. I,

16 A network "flow" describes established network connections through which network packets flow. The flow data store maintains information about each flow, including source, destination, volume of bytes that have been transferred in that flow, and other

17

REDACTED Ex. A Ex. F

source code, and even declarations made by Symantec's own experts, supports the reasonable inference that products practice the claimed statistical profile inventions.

The inference of infringement finds its strongest support in Symantec documents identified by Dr. Kesidis in his expert report and during his deposition. These documents provide evidence that REDACTED performs every step of the asserted method claims of the '338 patent. For example, the evidence shows,

its ciscoworker and sniffworker software routines, receives packet data from the plurality

[Ex. E,

[Ex. T,

[Ex. T,

REDACTED

Ex. C

REDACTED

[Ex. T,

[Ex. W,

---

[18] Symantec criticizes Dr. Kesidis for relying on documents describing prior versions of REDACTED Yet Symantec and its experts have not provided a single suggestion that these documents do not accurately reflect the later versions or that the functionality described in them was materially changed in any way in later software releases.

Ex. X,

REDACTED

[*See* Ex. V

Thus, the documentation supports the inference that

infringe the asserted '338 patent claims.

In addition to these documents, the evidence of record includes source code

Ex. E

Ex. W,

REDACTED

See Ex. E, at ¶ 48

---

[19] Source code evidence was buried in and obscured by countless, irrelevant source code modules provided by Symantec at the escrow site. The escrow computer also contained empty directories, such as one named "flowchaser," which gave the impression that the flowchaser source code was not produced, making the systematic examination of the poorly documented code even more difficult. Additional source code evidence, however, was ultimately not necessary because sufficient evidence of infringement could be found in Symantec's other documentation.

[20]

REDACTED

REDACTED

To counter the evidence in Symantec's own documents, the source code, and the testimony, Symantec

REDACTED

Clearly, a question of fact exists, and a jury should be allowed not only to weigh the credibility of Dr. Hansen himself, but also the evidence in Symantec's own documents and Dr. Kesidis' interpretation of them. Because sufficient evidence exists to support a reasonable conclusion that the asserted claims of the '338 patent – and the "statistical detection" limitations of the '212 and '615 patents – . REDACTED

Symantec's motion as to these issues must be denied.

III. CONCLUSION

For the foregoing reasons, SRI respectfully requests that Symantec's Summary Judgment Motion of Non-Infringement be denied in its entirety.

REDACTED [Ex. Y

[21] Dr. Hansen admitted during his deposition that he did not in fact collect the particular source code himself; it was selected and provided to him by Mr. Bennett. [*See* Ex. V, at 36:18-37:13; 112:17-113:23].

Dated: June 30, 2006

FISH & RICHARDSON P.C.

By: */s/ John F. Horvath*

John F. Horvath (#4557)
Kyle Wagner Compton (#4693)
919 N. Market St., Ste. 1100
P.O. Box 1114
Wilmington, DE 19889-1114
Telephone: (302) 652-5070
Facsimile: (302) 652-0607

Howard G. Pollack (CA Bar No. 162897)
Katherine D. Prescott (CA Bar No. 215496)
500 Arguello St., Ste. 500
Redwood City, CA 94063
Telephone: (650) 839-5070
Facsimile: (650) 839-5071

Attorneys for Plaintiff/Counterclaim Defendant
SRI INTERNATIONAL, INC.

50355898.doc

CERTIFICATE OF SERVICE

I hereby certify that on July 10, 2006, I electronically filed the **REDACTED – SRI INTERNATIONAL, INC.'S RESPONSE TO SYMANTEC'S SUMMARY JUDGMENT MOTION OF NON-INFRINGEMENT** with the Clerk of Court the attached document using CM/ECF which will send electronic notification of such filing(s) to the following Delaware counsel.

Richard L. Horwitz
Potter Anderson & Corroon LLP
Hercules Plaza
1313 North Market Street, 6th Floor
P.O. Box 951
Wilmington, DE 19899

Attorneys for Defendant-Counterclaimant Internet Security Systems, Inc., a Delaware corporation, and Internet Security Systems, Inc., a Georgia corporation

Richard K. Herrmann
Morris James Hitchens & Williams
PNC Bank Center
222 Delaware Avenue, 10th Floor
P.O. Box 2306
Wilmington, DE 19899-2306

Attorneys for Defendant-Counterclaimant Symantec Corporation

/s/ *John F. Horvath*
John F. Horvath

80034097.doc